Amendments to the Claims

Kindly amend independent claims 1, 14, 27 & 28 and cancel claims 12 & 18 (without prejudice) as set forth below. All pending claims are reproduced below, with changes in the amended claims shown by underlining (for added matter) and strikethrough/double brackets (for deleted matter).

1.   (Currently Amended) A method for protecting a stream of data to be transferred between an encryption unit and a decryption unit, said method comprising:

encrypting the stream of data at said encryption unit for transferring of said encrypted stream of data from said encryption unit to said decryption unit;

dynamically varying said encrypting of said stream of data at said encryption unit over multiple portions of the stream of data by dynamically changing simultaneously multiple encryption parameters employed for each portion of the stream of data and signaling said dynamic change in encryption parameters to said decryption unit, said dynamically varying of said multiple encryption parameter parameters employed for each portion of the stream of data being responsive to occurrence of a predefined condition in said stream of data; and

decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said dynamically changed, multiple encryption parameters.

2.   (Previously Presented) The method of claim 1, wherein said multiple encryption parameters comprise at least two of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

3.   (Canceled).

4.   (Previously Presented) The method of claim 2, further comprising multiplexing said changed encryption parameters and said encrypted data at a sender prior to transferring thereof to a receiver containing said decryption unit, and demultiplexing said changed encryption parameters and said encrypted data at said receiver.

5.   (Previously Presented) The method of claim 1, wherein said dynamically varying comprises dynamically varying said multiple encryption parameters based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

6.   (Canceled).

7.   (Original) The method of claim 1, wherein said stream of data comprises a stream of compressed data, and wherein said method further comprises decompressing said compressed data after said decrypting of said encrypted data by said decryption unit.

8.   (Previously Presented) The method of claim 7, wherein said stream of compressed data comprises one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

9.   (Previously Presented) The method of claim 1, further comprising initializing a plurality of encryption parameters based on a sensitivity of said stream of data, said plurality of encryption parameters being employed by said encrypting and wherein said changed multiple encryption parameters of said dynamically varying comprise multiple encryption parameters of said plurality of encryption parameters.

10.   (Previously Presented) The method of claim 1, wherein said stream of data comprises a stream of MPEG compressed data, and said method further comprises setting a plurality of encryption parameters for use by said encrypting based upon sensitivity of said stream of MPEG compressed data, and wherein said changed multiple encryption parameters comprise multiple encryption parameters of said plurality of encryption parameters.

11.   (Previously Presented) The method of claim 10, wherein said setting of said plurality of encryption parameters includes establishing at least two of an encryption granularity, an initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger for said stream of MPEG encoded data.

12.   (Canceled).

13.   (Previously Presented) The method of claim 1, wherein said dynamically varying comprises dynamically varying said multiple encryption parameters responsive to passage of a predefined number of data bits in said stream of data, or alternatively, responsive to passage of a predefined number of data units in said stream of data, wherein said data units comprise at least one of a program, a sequence, a group of pictures, a picture, a slice, or a macroblock.

14.   (Currently Amended) A system for protecting a stream of data comprising:

an encryption unit and a decryption unit, the encryption unit encrypting the stream of data for transfer to the decryption unit;

means for dynamically varying said encrypting of said stream of data by said encryption unit over multiple portions of the stream of data by dynamically changing simultaneously multiple encryption parameters employed by each portion of the stream of data and signaling said dynamic change in encryption parameters employed by each portion of the stream of data to said decryption unit, said means for dynamically varying being responsive to occurrence of a predefined condition in said stream of data; and

wherein said decryption unit decrypts said encrypted data, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said dynamically changed, multiple encryption parameters.

15.   (Canceled).

16.   (Previously Presented) The system of claim 14, wherein said stream of data comprises a stream of digital data.

17.   (Previously Presented) The system of claim 14, wherein said means for dynamically varying comprises means for dynamically varying said multiple encryption parameters based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

18.   (Canceled).

19.   (Previously Presented) The system of claim 14, wherein said multiple encryption parameters comprise at least two of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

20.   (Canceled).

21.   (Previously Presented) The system of claim 14, further comprising a data multiplexer for multiplexing said changed encryption parameters into said encrypted data for transfer thereof to said decryption unit.

22.   (Previously Presented) The system of claim 14, further comprising means for setting a plurality of encryption parameters based on sensitivity of said stream of data, said plurality of encryption parameters being employed by said encryption unit and wherein said changed multiple encryption parameters comprise encryption parameters of said plurality of encryption parameters.

23.   (Original) The system of claim 22, wherein said stream of data comprises a stream of compressed data, and wherein said system further comprises a decoder for decompressing said compressed data after decrypting thereof by said decryption unit.

24.   (Previously Presented) The system of claim 23, wherein said stream of compressed data comprises a stream of one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

25.   (Previously Presented) The system of claim 22, wherein said means for setting said plurality of encryption parameters includes means for establishing at least two of an encryption granularity, an encryption key, a density scale, a density, an encryption delay, and a key update data trigger.

26.   (Previously Presented) The system of claim 14, wherein said means for dynamically varying comprises means for changing said multiple encryption parameters based on a predefined number of bits being encoded by said encryption unit, or alternatively, based on a predefined number of units being encoded by said encryption unit, said units comprising one of a program, a sequence, a group of pictures, a picture, a slice, or a macroblock.

27.   (Currently Amended) A system for protecting a stream of data to be transferred between a sender and a receiver, said system comprising:

an encryption unit disposed at said sender for encrypting the stream of data prior to transfer to said receiver, said encryption unit being adapted to dynamically vary encrypting of the stream of data over multiple portions of the stream of data by dynamically changing simultaneously multiple encryption parameters employed for each portion of the stream of data based on an occurrence of a predefined condition in said data stream and signaling said change in encryption parameters employed for each portion of the stream of data to said receiver; and

a decryption unit disposed at said receiver for decrypting said encrypted data, said decryption unit being adapted to receive said changed encryption parameters to account for said dynamic varying of said encrypting by said encryption unit using said changed encryption parameters.

28.   (Currently Amended) At least one program storage device readable by a machine, tangibly embodying at least one program of instructions executable by the machine to perform a method for protecting a stream of data to be transferred between an encryption unit and a decryption unit, comprising;

encrypting the stream of data at said encryption unit for transfer thereof to said decryption unit;

dynamically varying said encrypting of said stream of data at said encryption unit over multiple portions of the stream of data by dynamically changing ~~simultaneously~~ multiple encryption parameters employed for each portion of the stream of data and signaling said change in encryption parameters to said decryption unit, wherein said dynamically varying of said multiple encryption parameters employed for each portion of the stream of data is responsive to occurrence of a predefined condition in said stream of data; and

decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said dynamically changed, multiple encryption parameters.

29.   (Previously Presented) The at least one program storage device of claim 28, wherein said multiple encryption parameters comprise at least two of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

30.   (Canceled).

31.   (Previously Presented) The at least one program storage device of claim 29, wherein said method further comprises multiplexing said changed encryption parameters and said encrypted data at a sender prior to transferring thereof to a receiver containing said decryption unit, and demultiplexing said changed encryption parameters and said encrypted data at said receiver.

32.   (Previously Presented) The at least one program storage device of claim 28, wherein said dynamically varying comprises dynamically varying said multiple encryption parameters based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

33.   (Canceled).

34.   (Original) The at least one program storage device of claim 28, wherein said stream of data comprises a stream of compressed data, and wherein said method further comprises decompressing said compressed data after said decrypting of said encrypted data by said decryption unit.

35.   (Previously Presented) The at least one program storage device of claim 34, wherein said stream of compressed data comprises one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

36.   (Previously Presented) The at least one program storage device of claim 28, wherein said method further comprises initializing a plurality of encryption parameters based on sensitivity of said stream of data, said plurality of encryption parameters being employed by said encrypting and wherein said changed multiple encryption parameters of said dynamically varying comprise multiple encryption parameters of said plurality of encryption parameters.

37.   (Previously Presented) The at least one program storage device of claim 28, wherein said stream of data comprises a stream of MPEG compressed data, and said method further comprises setting a plurality of encryption parameters for use by said encrypting based upon sensitivity of said stream of MPEG compressed data, and wherein said changed multiple encryption parameters comprise multiple encryption parameters of said plurality of encryption parameters.

38.   (Previously Presented) The at least one program storage device of claim 37, wherein said setting of said plurality of encryption parameters includes establishing at least two of an encryption granularity, an initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger for said stream of MPEG encoded data.

* * * * *